

ENCRYPTION AND DECRYPTION APPARATUS, ENCRYPTION AND DECRYPTION METHOD AND THEIR PROGRAM MEMORY MEDIUM

Publication number: JP2000066585

Publication date: 2000-03-03

Inventor: KAWAMURA SHINICHI; SANO FUMIHIKO

Applicant: TOKYO SHIBAURA ELECTRIC CO

Classification:




- International: **G09C1/00; H04L9/06; G09C1/00; H04L9/06; (IPC1-7): G09C1/00; H04L9/06**

- european: **H04L9/06C**

Application number: JP19980233921 19980820

Priority number(s): JP19980233921 19980820

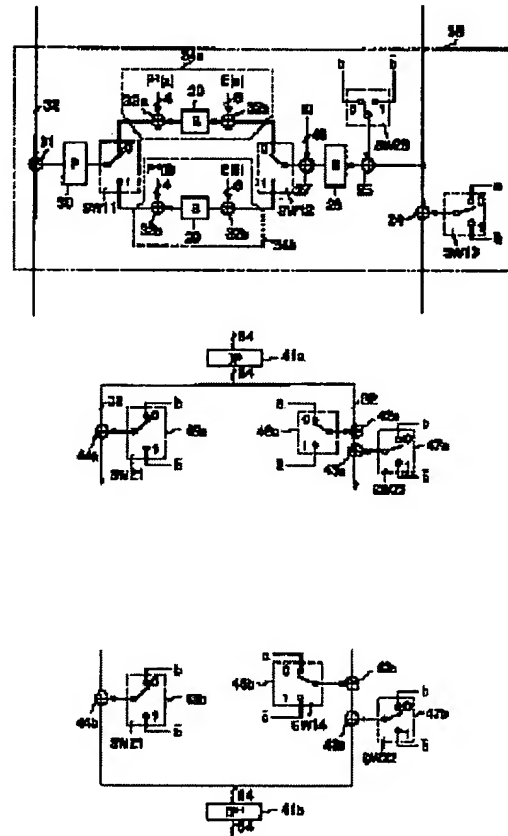
Also published as:

 EP0981223 (A2)
 US6940975 (B1)
 EP0981223 (A3)

[Report a data error here](#)

Abstract of JP2000066585

PROBLEM TO BE SOLVED: To provide a means which makes the cryptanalysis by a DPA (differential power analysis) difficult without changing the results of the data encryption processing of the conventional encryption apparatus, decryption apparatus, encryption means and decryption means. **SOLUTION:** Each stage function of a data agitation section is provided with a pair of the pattern of a mask (a) and the mask pattern which is a reversal of its bit. One of the pair is randomly selected by a switch SW12 every time when encryption is executed to obtain the exclusive-OR 32a of the input to an S box 29 and the selected mask pattern and to obtain the exclusive-OR 33a of the output of the S box 29 and the bit of the reverse transposition P-1 of the mask (a). The exclusive-ORs 32a, 33a are previously calculated and are recorded as a table in the S box 29. Further, the output of each stage function 5 is subjected to the exclusive-OR 43a with the mask (b) and is concealed. The influence by the mask (b) is eliminated by executing the exclusive-OR with the mask (b) again in the ensuing stage.



Data supplied from the **esp@cenet** database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-66585

(P2000-66585A)

(43) 公開日 平成12年3月3日 (2000.3.3)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00	6 1 0 B 5 K 0 1 3
H 0 4 L 9/06		H 0 4 L 9/00	6 1 1 A

審査請求 未請求 請求項の数54 O L (全 18 頁)

(21) 出願番号 特願平10-233921

(22) 出願日 平成10年8月20日 (1998.8.20)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 川村 信一

東京都府中市東芝町1番地 株式会社東芝
府中工場内

(72) 発明者 佐野 文彦

東京都府中市東芝町1番地 株式会社東芝
府中工場内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

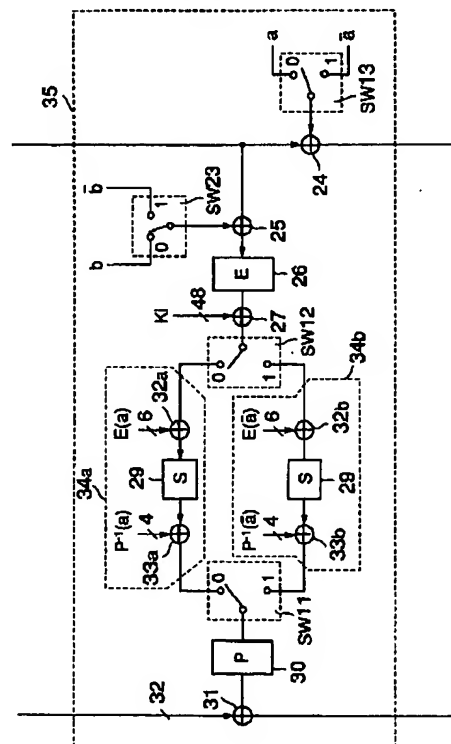
Fターム(参考) 5K013 CA04 CA07 CA14 DA02

(54) 【発明の名称】 暗号化・復号装置、暗号化・復号方法、およびそのプログラム記憶媒体

(57) 【要約】

【課題】従来の暗号化装置、復号装置、暗号化手段、および復号手段のデータ暗号処理結果を変更することなく、DPAによる解読を困難にする手段を提供する。

【解決手段】データ攪拌部1の各段関数5において、マスクaのパターンとそのビット反転のマスクパターンのペアが設けられる。暗号化を行う毎にこのペアの一方をスイッチSW12によりランダムに選択し、S箱29への入力と選択したマスクパターンとの排他的論理和32aが取られると共に、S箱29の出力と、マスクaの逆転置P⁻¹のビットとの排他的論理和33aが取られる。排他的論理和32a、33aは事前に計算されテーブルとしてS箱29に記録される。さらに、各段関数5の出力はマスクbと排他的論理和43aが取られ、秘匿される。このマスクbによる影響は次段において、再度マスクbと排他的論理和を取ることでマスクbによる影響を除去する。



【特許請求の範囲】

【請求項1】 平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換する暗号化装置であって、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^{-}) (i は1以上の正の整数)の中から一方を、暗号化を行う毎にランダムに選択する手段と、装置内部の平文に依存したビットを、前記選択手段により選択されたマスクパターンによってマスクする手段と、暗号文を出力する前に、暗号文から前記マスク a の影響を除去する手段とを具備したことを特徴とする暗号化装置。

【請求項2】 平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換する暗号化装置であって、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^{-}) (i は1以上の正の整数)の中から一方を、暗号化を行う毎にランダムに選択する手段と、装置内部の中間的なビットデータを、前記選択手段により選択されたマスクパターンによってマスクする手段と、前記マスク手段によりマスクされた中間的なビットデータから前記マスク a の影響を除去する手段とを具備したことを特徴とする暗号化装置。

【請求項3】 平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換する暗号化装置であって、装置内部の中間的なデータに対してデータ変換を行うデータ変換手段と、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^{-}) (i は1以上の正の整数)の中から一方を、暗号化を行う毎にランダムに選択する手段と、前記データ変換手段の入力を、前記選択手段により選択されたマスクパターンによってマスクする手段と、前記マスク手段によりマスクされた、前記データ変換手段の出力から前記マスク a の影響を除去する手段とを具備したことを特徴とする暗号化装置。

【請求項4】 前記装置内部の平文に依存したビットを選択されたマスクパターンによってマスクする手段、および前記暗号文から該マスク a の影響を除去する手段が、排他的論理和、定数 w を法とする加算または減算、および定数 w を法とする乗算または除算のいずれかで構成されることを特徴とする請求項1記載の暗号化装置。

【請求項5】 前記装置内部の中間的なビットデータを選択されたマスクパターンによってマスクする手段、およびマスクされた中間的なビットデータから該マスク a の影響を除去する手段は、排他的論理和、定数 w を法とする加算または減算、および定数 w を法とする乗算または除算のいずれかで構成されることを特徴とする請求項

2記載の暗号化装置。

【請求項6】 前記データ変換手段、前記データ変換手段の入力を前記選択されたマスクパターンによってマスクする手段、および前記マスクされたデータの変換手段の出力から該マスク a の影響を除去する手段は、排他的論理和、定数 w を法とする加算または減算、および定数 w を法とする乗算または除算のいずれかで構成されることを特徴とする請求項3記載の暗号化装置。

【請求項7】 前記データ変換手段は、ビット入れ替えに相当する変換手段またはビット換字に相当する手段のいずれかで構成されることを特徴とする請求項3の暗号化装置。

【請求項8】 前記あらかじめ定められたひとつ又は複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^{-}) (i は1以上の正の整数)の中から一方を、暗号化を行う毎にランダムに選択する手段と、前記データ変換手段の入力を、前記マスクパターン a_i によってマスクする手段と、および前記マスクされた、前記データ変換手段の出力から前記マスク a_i の影響を除去する手段と、をテーブル形式で記憶する第1の記憶手段と、

前記データ変換手段の入力をマスクパターン a_i^{-} によってマスクする手段と、

前記マスクされた前記データ変換手段の出力から前記マスク a_i^{-} の影響を除去する手段と、をテーブル形式で記憶する第2の記憶手段と、

前記第1の記憶手段と第2の記憶手段の一方を、暗号化を行う毎にランダムに選択し、マスクされたデータに対して前記データ変換手段の処理を行う、マスクされたデータの変換手段とをさらに有することを特徴とする請求項3記載の暗号化装置。

【請求項9】 前記マスクパターンとそのビット反転のマスクパターンのペア (a , a^{-}) が、あらかじめ定められた固定のマスクパターンとそのビット反転のマスクパターンのペア (a , a^{-}) で構成されることを特徴とする請求項1記載の暗号化装置。

【請求項10】 前記マスクパターンとそのビット反転のマスクパターンのペア (a , a^{-}) が、必ずしも秘密でないことを特徴とする請求項1記載の暗号化装置。

【請求項11】 n ビット長のビット列 x の1のビットの数を示すハミング重みを $H(x)$ と定義し、前記マスク a のハミング重み $H(a)$ が $0 < H(a) < n$ を満足することを特徴とする請求項1記載の暗号化装置。

【請求項12】 n ビット長のビット列 x の1のビットの数を示すハミング重みを $H(x)$ と定義し、前記マスク a のハミング重み $H(a)$ と、前記マスク a のビット反転 a^{-} のハミング重み $H(a^{-})$ の差の絶対値が、 $n/2$ 未満であることを特徴とする請求項1記載の暗号化装置。

【請求項13】 暗号ブロックを与えられた鍵情報に依

存して平文ブロックに変換する復号装置であって、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^-) (i は1以上の正の整数)の中から一方を、復号を行う毎にランダムに選択する手段と、

装置内部の暗号文に依存したビットを、前記選択手段により選択されたマスクパターンによってマスクする手段と、

平文を出力する前に、前記平文から前記マスク a の影響を除去する手段とを具備したことを特徴とする復号装置。

【請求項14】 暗号ブロックを与えられた鍵情報に依存して平文ブロックに変換する復号装置であって、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^-) (i は1以上の正の整数)の中から一方を、復号を行う毎にランダムに選択する手段と、装置内部の中間的なビットデータを、前記選択手段により選択されたマスクパターンによってマスクする手段と、

前記マスク手段によりマスクされた中間的なビットデータから前記マスク a の影響を除去する手段とを具備したことを特徴とする復号装置。

【請求項15】 暗号ブロックを与えられた鍵情報に依存して平文ブロックに変換する復号装置であって、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^-) (i は1以上の正の整数)の中から一方を、復号を行う毎にランダムに選択する手段と、前記データ変換手段の入力を、前記選択手段により選択されたマスクパターンによってマスクする手段と、前記マスク手段によりマスクされた、前記データ変換手段の出力から前記マスク a の影響を除去する手段とを具備したことを特徴とする復号装置。

【請求項16】 前記装置内部の暗号文に依存したビットを選択されたマスクパターンによってマスクする手段と、該暗号文から該マスク a の影響を除去する手段とが、排他的論理和、定数 w を法とする加算または減算、および定数 w を法とする乗算または除算のいずれかで構成されることを特徴とする請求項13記載の復号装置。

【請求項17】 前記装置内部の中間的なビットデータを選択されたマスクパターンによってマスクする手段と、マスクされた中間的なビットデータから該マスク a の影響を除去する手段とが、排他的論理和、定数 w を法とする加算または減算、および定数 w を法とする乗算または除算のいずれかで構成されることを特徴とする請求項14記載の復号装置。

【請求項18】 前記データ変換手段と、前記選択されたマスクパターンを用いて、前記第1のデータ変換手段の入力を選択されたマスクパターンによってマスクする

手段と、前記マスクされた第1のデータ変換手段の出力から該マスク a の影響を除去する手段とが、排他的論理和、定数 w を法とする加算または減算、および定数 w を法とする乗算または除算のいずれかで構成されることを特徴とする請求項15記載の復号装置。

【請求項19】 前記データ変換手段は、ビット入れ替えに相当する変換手段またはビット換字に相当する手段のいずれかで構成されることを特徴とする請求項15の暗号化装置。

【請求項20】 あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^-) (i は1以上の正の整数)の中から一方を、復号を行う毎にランダムに選択する手段と、

前記データ変換手段の入力をマスクパターン a_i によってマスクする手段と、

前記マスクされた該データ変換手段の出力から前記マスク a_i の影響を除去する手段、をテーブル形式で記憶する第1の記憶手段と、

前記データ変換手段の入力をマスクパターン a_i^- によってマスクする手段と、

前記マスクされた該データ変換手段の出力から前記マスク a_i^- の影響を除去する手段と、をテーブル形式で記憶する第2の記憶手段と、

前記第1の記憶手段と第2の記憶手段の一方を、暗号化を行う毎にランダムに選択し、マスクされたデータに対して前記データ変換手段の処理を行うマスクされたデータの変換手段とをさらに有することを特徴とする請求項15記載の復号装置。

【請求項21】 前記マスクパターンとそのビット反転のマスクパターンのペア (a_i , a_i^-) が、あらかじめ定められた固定のマスクパターンとそのビット反転のマスクパターンのペア (a_i , a_i^-) であることを特徴とする請求項13記載の復号装置。

【請求項22】 前記マスクパターンとそのビット反転のマスクパターンのペア (a_i , a_i^-) が、必ずしも秘密でないことを特徴とする請求項13記載の復号装置。

【請求項23】 n ビット長のビット列 x の1のビットの数を示すハミング重みを $H(x)$ と定義し、前記マスク a のハミング重み $H(a)$ が、 $0 < H(a) < n$ を満足することを特徴とする請求項13記載の復号装置。

【請求項24】 n ビット長のビット列 x の1のビットの数を示すハミング重みを $H(x)$ と定義し、前記マスク a のハミング重み $H(a)$ と、前記マスク a のビット反転 a^- のハミング重み $H(a^-)$ の差の絶対値が、 $n/2$ 未満であることを特徴とする請求項13記載の復号装置。

【請求項25】 平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換する暗号化方法であって、

あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^-) (i は1以上の正の整数)の中から一方を、暗号化を行う毎にランダムに選択するステップと、前記選択されたマスクパターンを用いて、方法内部の平文に依存したビットを選択されたマスクパターンによってマスクするステップと、暗号文を出力する前に、暗号文から前記マスク a の影響を除去するステップとを具備したことを特徴とする暗号化方法。

【請求項26】 平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換する暗号化方法であって、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^-) (i は1以上の正の整数)の中から一方を、暗号化を行う毎にランダムに選択するステップと、方法内部の中間的なビットデータを前記選択されたマスクパターンによってマスクするステップと、前記マスクされた中間的なビットデータから前記マスク a の影響を除去するステップとを具備したことを特徴とする暗号化方法。

【請求項27】 平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換する暗号化方法であって、方法内部の中間的なデータにデータ変換を行うデータ変換ステップと、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^-) (i は1以上の正の整数)の中から一方を、暗号化を行う毎にランダムに選択するステップと、前記選択されたマスクパターンを用いて、前記データ変換ステップの入力を選択されたマスクパターンによってマスクするステップと、前記マスクされたデータ変換ステップの出力から前記マスク a の影響を除去するステップとを具備したことを特徴とする暗号化方法。

【請求項28】 前記方法内部の平文に依存したビットを前記選択されたマスクパターンによってマスクするステップと、前記暗号文から前記マスク a の影響を除去するステップとが、排他的論理和、定数 w を法とする加算または減算、および定数 w を法とする乗算または除算のいずれかで構成されることを特徴とする請求項25記載の暗号化方法。

【請求項29】 前記選択されたマスクパターンを用いて、方法内部の中間的なビットデータを前記選択されたマスクパターンによってマスクするステップと、前記マスクされた中間的なビットデータから前記マスク a の影響を除去するステップとが、排他的論理和、定数 w を法とする加算または減算、および定数 w を法とする乗算または除算のいずれかで構成されることを特徴とする請求項26記載の暗号化方法。

【請求項30】 前記データ変換ステップと、前記選択されたマスクパターンを用いて、前記第1のデータ変換ステップの入力を前記選択されたマスクパターンによってマスクするステップと、前記マスクされたデータ変換ステップの出力から前記マスク a の影響を除去するステップとが、排他的論理和、定数 w を法とする加算または減算、および定数 w を法とする乗算または除算のいずれかで構成されることを特徴とする請求項27記載の暗号化方法。

【請求項31】 前記データ変換ステップは、ビット入れ替えに相当する変換ステップまたはビット換字に相当するステップのいずれかであることを特徴とする請求項27記載の暗号化方法。

【請求項32】 あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^-) (i は1以上の正の整数)の中から一方を、暗号化を行う毎にランダムに選択するステップと、前記データ変換ステップの入力をマスクパターン a_i によってマスクするステップと、前記マスクされた前記データ変換ステップの出力から前記マスク a_i の影響を除去するステップとをテーブル形式で記憶する第1の記憶ステップと、前記データ変換ステップの入力をマスクパターン a_i^- によってマスクするステップと、前記マスクされた前記データ変換ステップの出力から前記マスク a_i^- の影響を除去するステップとをテーブル形式で記憶する第2の記憶ステップと、前記第1の記憶ステップと第2の記憶ステップの一方を、暗号化を行う毎にランダムに選択しマスクされたデータに対して前記データ変換ステップの処理を行う、マスクされたデータの変換ステップとをさらに有したことを特徴とする請求項27記載の暗号化方法。

【請求項33】 前記マスクパターンとそのビット反転のマスクパターンのペア (a_i , a_i^-) が、あらかじめ定められた固定のマスクパターンとそのビット反転のマスクパターンのペア (a_i , a_i^-) で構成されることを特徴とする請求項25記載の暗号化方法。

【請求項34】 前記マスクパターンとそのビット反転のマスクパターンのペア (a_i , a_i^-) が、必ずしも秘密でないことを特徴とする請求項25記載の暗号化方法。

【請求項35】 n ビット長のビット列 x の1のビットの数を示すハミング重みを $H(x)$ と定義し、前記マスク a のハミング重み $H(a)$ が $0 < H(a) < n$ を満足することを特徴とする請求項25記載の暗号化方法。

【請求項36】 n ビット長のビット列 x の1のビットの数を示すハミング重みを $H(x)$ と定義し、前記マスク a のハミング重み $H(a)$ と、前記マスク a のビット反転 a^- のハミング重み $H(a^-)$ の差の絶対値が $n/$

2未満であることを特徴とする請求項25記載の暗号化方法。

【請求項37】 暗号ブロックを与えられた鍵情報に依存して平文ブロックに変換する復号方法であって、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^{-1}) (i は1以上の正の整数)の中から一方を、復号を行う毎にランダムに選択するステップと、前記選択されたマスクパターンを用いて、方法内部の暗号文に依存したビットを選択されたマスクパターンによってマスクするステップと、平文を出力する前に、平文から前記マスク a の影響を除去するステップと、を具備したことを特徴とする復号方法。

【請求項38】 暗号ブロックを与えられた鍵情報に依存して平文ブロックに変換する復号方法であって、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^{-1}) (i は1以上の正の整数)の中から一方を、復号を行う毎にランダムに選択するステップと、前記選択されたマスクパターンを用いて、方法内部の中間的なビットデータを選択されたマスクパターンによってマスクするステップと、前記マスクされた中間的なビットデータから前記マスク a の影響を除去するステップとを具備したことを特徴とする復号方法。

【請求項39】 暗号ブロックを与えられた鍵情報に依存して平文ブロックに変換する復号方法であって、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^{-1}) (i は1以上の正の整数)の中から一方を、復号を行う毎にランダムに選択するステップと、前記選択されたマスクパターンを用いて、前記データ変換ステップの入力を選択されたマスクパターンによってマスクするステップと、前記マスクされたデータの変換ステップの出力から前記マスク a の影響を除去するステップとを具備したことを特徴とする復号方法。

【請求項40】 前記方法内部の暗号文に依存したビットを選択されたマスクパターンによってマスクするステップと、前記暗号文から該マスク a の影響を除去するステップとが、排他的論理和、定数 w を法とする加算または減算、および定数 w を法とする乗算または除算のいずれかで構成されることを特徴とする請求項37記載の復号方法。

【請求項41】 前記選択されたマスクパターンを用いて、方法内部の中間的なビットデータを選択されたマスクパターンによってマスクするステップと、前記マスクされた中間的なビットデータから該マスク a の影響を除去するステップとが、排他的論理和、定数 w を法とする

加算または減算、および定数 w を法とする乗算または除算のいずれかで構成されることを特徴とする請求項38記載の復号方法。

【請求項42】 前記データ変換ステップと、前記選択されたマスクパターンを用いて、前記第1のデータ変換ステップの入力を選択されたマスクパターンによってマスクするステップと、前記マスクされた第1のデータ変換ステップの出力から該マスク a の影響を除去するステップとが、排他的論理和、定数 w を法とする加算または減算、および定数 w を法とする乗算または除算のいずれかで構成されることを特徴とする請求項39記載の復号方法。

【請求項43】 前記データ変換ステップは、ビット入れ替えに相当する変換ステップまたはビット換字に相当するステップのいずれかであることを特徴とする請求項39記載の暗号化方法。

【請求項44】 あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i , a_i^{-1}) (i は1以上の正の整数)の中から一方を、復号を行う毎にランダムに選択するステップと、前記データ変換ステップの入力をマスクパターン a_i によってマスクするステップと、前記マスクされた前記データ変換ステップの出力から前記マスク a_i の影響を除去するステップとをテーブル形式で記憶する第1の記憶ステップと、

前記データ変換ステップの入力をマスクパターン a_i^{-1} によってマスクするステップと、前記マスクされた該データ変換ステップの出力から該マスク a_i^{-1} の影響を除去するステップとをテーブル形式で記憶する第2の記憶ステップと、

前記第1の記憶ステップと第2の記憶ステップの一方を、暗号化を行う毎にランダムに選択し、マスクされたデータに対して前記データ変換ステップの処理を行う、マスクされたデータの変換ステップとをさらに有することを特徴とする請求項39記載の復号方法。

【請求項45】 前記マスクパターンとそのビット反転のマスクパターンのペア (a_i , a_i^{-1}) が、あらかじめ定められた固定のマスクパターンとそのビット反転のマスクパターンのペア (a_i , a_i^{-1}) であることを特徴とする請求項37記載の復号方法。

【請求項46】 前記マスクパターンとそのビット反転のマスクパターンのペア (a_i , a_i^{-1}) が、必ずしも秘密でないことを特徴とする請求項37記載の復号方法。

【請求項47】 n ビット長のビット列 x の1のビットの数を示すミング重みを $H(x)$ と定義し、前記マスク a のハミング重み $H(a)$ が $0 < H(a) < n$ を満足することを特徴とする請求項37記載の復号方法。

【請求項48】 n ビット長のビット列 x の1のビットの数を示すミング重みを $H(x)$ と定義し、前記マスク

aのハミング重み $H(a)$ と、前記マスクaのビット反転 a^- のハミング重み $H(a^-)$ の差の絶対値が、 $n/2$ 未満であることを特徴とする請求項37記載の復号方法。

【請求項49】 平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換させるための、コンピュータ読み出し可能なプログラムコード手段が記憶されたコンピュータ使用可能なプログラム記憶媒体であって、コンピュータに、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i, a_i^-) (i は1以上の正の整数)の中から一方を、暗号化を行う毎にランダムに選択させるためのコンピュータ読み出し可能なプログラムコード手段と、

コンピュータに、前記選択されたマスクパターンを用いて、方法内部の平文に依存したビットを選択されたマスクパターンによってマスクさせるためのコンピュータ読み出し可能なプログラムコード手段と、

コンピュータに、暗号文を出力する前に、暗号文から前記マスクaの影響を除去させるためのコンピュータ読み出し可能なプログラムコード手段とを具備したことを特徴とするプログラム記憶媒体。

【請求項50】 平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換する暗号化装置であって、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i, a_i^-) (i は1以上の正の整数)の中から一方を、暗号化を行う毎にランダムに選択する手段と、装置内部の鍵に依存したビットを、前記選択手段により選択されたマスクパターンによってマスクする手段と、装置内部の中間的なデータに対して鍵によってデータ変換を行うデータ変換手段と、

前記データ変換手段の出力から前記マスクaの影響を除去する手段とを具備したことを特徴とする暗号化装置。

【請求項51】 前記マスクパターンとそのビット反転のマスクパターンのペア (a, a^-) が、あらかじめ定められた固定のマスクパターンとそのビット反転のマスクパターンのペア (a, a^-) で構成されることを特徴とする請求項50記載の暗号化装置。

【請求項52】 前記マスクパターンとそのビット反転のマスクパターンのペア (a, a^-) が、必ずしも秘密でないことを特徴とする請求項50記載の暗号化装置。

【請求項53】 n ビット長のビット列 x の1のビットの数を示すハミング重みを $H(x)$ と定義し、前記マスクaのハミング重み $H(a)$ が $0 < H(a) < n$ を満足することを特徴とする請求項50記載の暗号化装置。

【請求項54】 n ビット長のビット列 x の1のビットの数を示すハミング重みを $H(x)$ と定義し、前記マスクaのハミング重み $H(a)$ と、前記マスクaのビット反転 a^- のハミング重み $H(a^-)$ の差の絶対値が、 n

$/2$ 未満であることを特徴とする請求項50記載の暗号化装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は暗号化装置、復号装置、暗号化手法、および復号手法に関し、特に、秘密鍵ブロック暗号を用いた暗号化装置、復号装置、暗号化手法、復号手法、およびそのプログラム記憶媒体に関する。

【0002】

【従来の技術】DES (Data Encryption Standard) は、現在、最も広範に用いられている秘密鍵ブロック暗号であり、特開昭51-108701号広報に詳細に記載されている。

【0003】DES に関してはさまざまな観点からの評価が行われており、差分解読法や線形解読法といった鍵の全数探索よりも効率的な解読法が提案された。

【0004】なお、差分解読法については、文献、E. Biham and A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Journal of CRYPTOLOGY, Vol. 4, Number 1, 1991 に、線形解読法については、文献、松井充、"DES 暗号の線形解読(1)"、暗号と情報セキュリティシンポジウム、SCIS93-3C, 1993に記載されている。

【0005】新たな解読方法としてDPA (Differential Power Analysis) が提案されている。DPA はデータのあるビットに着目して消費電力の差異(ビット0のときの消費電力とビット1のときの消費電力)を計測し、ビットを推測する。例えば、DES の場合、既知の暗号文出力と鍵の推測により、S 箱の入力およびそれに対応する出力を推測する。上記S 箱出力で推測した、ある1ビットが0あるいは1である場合の消費電力の差異を計測し、推測の正当性の検証、すなわち鍵の推測の正当性の検証を行う手法がDPA である。

【0006】

【発明が解決しようとする課題】このため、上述したDPAによりDESが解読される恐れがあり、さらなるセキュリティが求められていた。

【0007】本発明の目的は、従来の暗号化装置、復号装置、暗号化手法、および復号手法のデータ暗号化処理結果を変更することなく、DPA による解読を困難にする暗号化・復号装置、暗号化・復号方法、およびそのプログラム記憶媒体を提供することである。

【0008】

【課題を解決するための手段】上述の課題を解決するため、本発明は、平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換する暗号化装置において、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i, a_i^-) (i は1以上の正の整数)の中から一方を、暗号

化を行う毎にランダムに選択する手段と、装置内部の平文に依存したビットを、前記選択手段により選択されたマスクパターンによってマスクする手段と、暗号文を出力する前に、暗号文から前記マスクaの影響を除去する手段とを具備したことを特徴とする。

【0009】また、本発明は、暗号ブロックを与えられた鍵情報に依存して平文ブロックに変換する復号装置において、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i, a_i^-) (i は1以上の正の整数)の中から一方を、復号を行う毎にランダムに選択する手段と、装置内部の暗号文に依存したビットを、前記選択手段により選択されたマスクパターンによってマスクする手段と、平文を出力する前に、前記平文から前記マスクaの影響を除去する手段とを具備したことを特徴とする。

【0010】また、本発明は、平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換する暗号化方法において、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i, a_i^-) (i は1以上の正の整数)の中から一方を、暗号化を行う毎にランダムに選択するステップと、前記選択されたマスクパターンを用いて、方法内部の平文に依存したビットを選択されたマスクパターンによってマスクするステップと、暗号文を出力する前に、暗号文から前記マスクaの影響を除去するステップとを具備したことを特徴とする。

【0011】また、この発明は、暗号ブロックを与えられた鍵情報に依存して平文ブロックに変換する復号方法において、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i, a_i^-) (i は1以上の正の整数)の中から一方を、復号を行う毎にランダムに選択するステップと、前記選択されたマスクパターンを用いて、方法内部の暗号文に依存したビットを選択されたマスクパターンによってマスクするステップと、平文を出力する前に、平文から前記マスクaの影響を除去するステップとを具備したことを特徴とする。

【0012】また、本発明は、平文ブロックを与えられた鍵情報に依存して暗号文ブロックに変換させるための、コンピュータ読み出し可能なプログラムコード手段が記憶されたコンピュータ使用可能なプログラム記憶媒体において、コンピュータに、あらかじめ定められたひとつまたは複数のマスクパターンとそのビット反転のマスクパターンの各ペア (a_i, a_i^-) (i は1以上の正の整数)の中から一方を、暗号化を行う毎にランダムに選択させるためのコンピュータ読み出し可能なプログラムコード手段と、コンピュータに、前記選択されたマスクパターンを用いて、方法内部の平文に依存したビットを選択されたマスクパターンによってマスクさせるためのコンピュータ読み出し可能なプログラムコード手段

と、コンピュータに、暗号文を出力する前に、暗号文から前記マスクaの影響を除去させるためのコンピュータ読み出し可能なプログラムコード手段とを具備したことを特徴とする。

【0013】この発明によれば、本来のデータをマスクし、各S箱に入力する直前でそのマスクを解除する。しかし、このマスクを解除したときに、DPAにより解読される恐れがある。このため、この発明によれば、S箱への入力直前におけるマスク解除、マスク解除後の本来のデータによるS箱への入力、およびS箱からの出力のマスク操作を、事前に計算し、テーブルとして記憶し、テーブルを参照することにより計算結果を求める。このため、暗号化および復号の処理中に、マスク解除のための排他的論理和の計算や、マスクをかけるための排他的論理和の計算が行われることはないので、DPAによる解読は不可能となる。

【0014】

【発明の実施形態】以下、図面を参照して本発明の実施形態を説明する。

【0015】図1は本発明が適用される、暗号化アルゴリズムDESの構成を示す図であり、平文(64ビット)3を外部から入力された鍵8に依存して攪拌し、対応する暗号文を出力する第1段〜第16段から構成されるデータ攪拌部1と、鍵情報kを前記データ攪拌部に供給される中間鍵に展開する鍵スケジュール部2からなる。

【0016】図1において、平文(64ビット)3は初期転置IP₄が施された後、2つに等分される。等分された結果の左側32ビットのデータと右側32ビットのデータはそれぞれ、段関数5の入力となる。段関数の構造は後述する。段関数の出力の左側32ビットのデータと右側32ビットのデータは入れ替えられて次段の段関数の入力となる。

【0017】上記段関数を16段繰り返した後、最終転置IP⁻¹₁₆により暗号文7が出力される。

【0018】図2は図1に示す段関数5の詳細ブロック図である。段関数17は転置E₁₁、排他的論理和13、S箱14、転置P₁₅および排他的論理和16とで構成される。

【0019】右側32ビットのデータを拡大転置E₁₁により48ビットに拡大し、その結果を排他的論理和13に出力する。排他的論理和13は、転置E₁₁の出力と、拡大鍵12の排他的論理和を出力する。排他的論理和13の出力48ビットは6ビットのデータに等分され、各S箱14の入力となる。この実施形態では、各S箱はテーブルで構成され、64エントリの6ビット入力に対してそれぞれ4ビットデータを出力する。例えばDESのS1は、6ビット入力の左端を第1ビット、右端を第6ビットとすると、第1ビットと第6ビットを2進数とみなした数字で図3に示すS箱の表の行を指定する。なお、図3に示すS箱の表の行番号は上から0、1、2、

3行と数える。次に残りの4ビットを2進数とみなした数字で列の番号を指定する。列番号も左端から0、1、2、3、…15列と数える。例えば、S1の入力を011011とすると、行番号は01すなわち、図3において、上から2番目の行となる。次に、列番号は01101すなわち13（左から14番目の列）なので表の値は5となる。従ってS1の出力はこの2進表現である0101となる。なお、図3では、S箱の出力を行と列で示したが、一般には、0から63までの入力に対応した表として構成される。各S箱の出力を結合した32ビットのデータは、転置P15によりビット転置操作が行われ、その結果が排他的論理和16に出力される。排他的論理和16は左側32ビットのデータと転置P15の出力との排他的論理和を出力する。

【0020】図4は図1に示す段関数5および図2に示す段関数17の詳細回路図であり、図5aは第1段の段関数への入力の構成を示す図であり、図5bは第16段の段関数の出力の構成を示す図である。

【0021】以下、図4、図5a、および図5bを参照して本発明の実施形態を詳細に説明する。

【0022】図4において、aおよびbはそれぞれ32ビットのマスクを表し、a[‐]はaの全ビット反転を表す。図4に示す段関数35において、排他的論理和25は、右側32ビットのデータを、スイッチSW23の出力と排他的論理和を行い拡大転置E26に出力する。拡大転置E26の出力は、排他的論理和27において拡大鍵Kiと排他的論理和が行われ、スイッチSW12に出力する。スイッチSW12は、後述の乱数列Rijによりデータの分岐を行う。例えば、Rijが0の場合には、スイッチSW12は、データを0側に分岐し、Rijが1の場合には、データを1側に分岐する。

【0023】図4において、スイッチSW12の分岐以降は、各S箱についての構成を示す図であり、すなわちS箱29はDESのS1～S8に対応する。

【0024】スイッチSW12が、データを0側に分岐した場合、破線34aで示す処理を行う。すなわち、排他的論理和32aは、排他的論理和27の出力と、マスクaに拡大転置Eを行った結果のS箱の入力に対応する6ビット(E(a))との排他的論理和を行い、その結果をS箱29に出力する。S箱29においては、対応するS箱のテーブル参照が行われた結果が、排他的論理和33aに出力される。

【0025】排他的論理和33aにおいては、マスクaに転置P30の逆転置P⁻¹を行った結果であるP⁻¹(a)のビットと、S箱29の出力との排他的論理和が行われ、その結果がスイッチSW11に出力される。

【0026】一方、スイッチSW12が、データを1側に分岐した場合、破線34bで示す処理を行う。すなわち、排他的論理和32bは、排他的論理和27の出力と、マスクa[‐]に拡大転置Eを行った結果のS箱の入力

に対応するビットとの排他的論理和を行い、その結果をS箱29に出力する。S箱29は、対応するS箱のテーブルを参照し、その結果を排他的論理和33bに出力する。

【0027】排他的論理和33bは、マスクa[‐]に転置P(30)の逆転置P⁻¹を行った結果であるP⁻¹(a[‐])のS箱の出力に対応する4ビットと、S箱29の出力との排他的論理和を行い、その結果をスイッチSW11に出力する。

【0028】ただし、上記破線34aおよび34bで示す各処理は、暗号化および復号の処理中に行ってはならない。なぜならば、上記マスクによるデータの秘匿を行っていても、S箱29の入出力は秘匿されていないため、S箱の処理の消費電力の差異を用いた解読が試みられる可能性があるからである。

【0029】本発明の実施形態では、破線34aおよび34bで示す各処理結果は、暗号化および復号を行う前に事前計算により処理結果を作成し、暗号化および復号処理を行う。例えば、各S箱について、S箱の入力のインデックスと出力を書き換えたテーブルを用意し、暗号化および復号の処理に用いる。このとき、マスクaに対応したS箱のテーブルとマスクa[‐]に対応したS箱のテーブルを用意する。例えば、マスクaを使って、図4の処理ブロック34aを計算した結果は以下の通りである。今、マスクaを(0110 1111 1100 1010 0110 1100 1100 0011)とする。拡大転置Eは図6に示す表で表される。図6の表において、各行は上からS1、S2、…S8への入力に対応する。また、各列は左端の第1ビットがS箱の入力の第1ビットに対応する。表の数字は拡大転置Eへの入力の第Xビットを表す。すなわち、S1の入力は、Eへの入力の第32、1、2、3、4、5ビットになる。従って、マスクaが上記の例の場合、S1の入力に対応するビットマスク(a)は(101101)となる。転置Pの表は図7に示される。図7において、左から順番にPの出力の第1ビットから第32ビットまでに対応する。(1行目と2行目は連続している)。各項目は入力の第Xビットを表す。すなわち、転置Pの出力の第1ビットは乳路y句の第16ビットになる。S1に対応するビットは転置Pの入力の第1、2、3、4ビットなので、それぞれPの出力の第9、17、23、31ビットに対応する。S1の出力に対応するマスクはP⁻¹(a)すなわち、Pの出力がaになる値なので、マスクaの第9、17、23、31ビットがP⁻¹(a)となる。従って、S1の出力に対応するマスクは(1001)となる。従って、マスクaが上記の場合、S1の入力に対応するビットマスクE(a)は(101101)、S1の出力に対応するビットマスクP⁻¹(a)は(1001)となる。実際に作成するマスクaに対応したテーブルは、入力をビットマスクE(a)と排他的

論理和した結果をS1の入力としてS1の出力を計算して、そのS1の出力にビットマスク $P^{-1}(a)$ を排他的論理和で加えたものがテーブルの出力になる。上記マスクaの場合、入力が(000000、000001、…111111)に対応する隠蔽されたS1の出力(0から63までの入力に対する出力)を列挙すると、それぞれの出力を列挙すると、図8に示すような結果となる。また、マスク a^{-} (aのビット反転)のテーブルは、図9に示すような結果となる。

【0030】破線34aおよび34bで示す各処理ブロックの出力は、転置P30において、転置が行われ排他的論理和31に出力される。排他的論理和31は、左側32ビットのデータと、転置P30の出力との排他的論理和を行う。排他的論理和24は右側32ビットのデータと、スイッチSW13の出力との排他的論理和を取り、新たな右側32ビットのデータとする。

【0031】図5aにおいて、平文(64ビット)を初期転置IP41aにより転置を行った結果は、等分され、右側32ビットと左側32ビットとなる。排他的論理和44aは、左側32ビットのデータと、スイッチSW21の出力との排他的論理和を取る。この排他的論理和44aの出力は、第1段の段関数の入力の左側32ビットとなる。排他的論理和42aは右側32ビットのデータと、スイッチSW14の出力との排他的論理和を取る。排他的論理和43aは、排他的論理和42aの出力と、スイッチSW22の出力との排他的論理和を取る。

【0032】この排他的論理和43aの出力は、第1段の段関数の入力の右側32ビットとなる。なお、図5aにおいて、排他的論理和の性質により42aと43aの順序は入れ替えても良い。

【0033】図5bにおいて、平文(64ビット)を初期転置IP41aにより転置を行った結果は、等分され、右側32ビットと左側32ビットとなる。排他的論理和44bは、左側32ビットのデータと、スイッチSW21の出力との排他的論理和を取る。これにより、図5aの排他的論理和43aにおいて加えたマスクの影響を除去する。排他的論理和44bの出力は、最終転置 $IP^{-1}41b$ に出力される。排他的論理和42bは、右側32ビットのデータと、スイッチSW14の出力との排他的論理和を取る。排他的論理和43bは、排他的論理和42bの出力と、スイッチSW22の出力との排他的論理和を取る。これにより、図5aの排他的論理和44aにおいて加えたマスクの影響を除去する。排他的論理和43bの出力は、最終転置 $IP^{-1}41b$ に出力される。なお、図5bにおいて、排他的論理和の性質により42bと43bの順序は入れ替えても良い。

【0034】図4、図5aおよび図5bで示した構成の特徴を以下に述べる。

【0035】排他的論理和44a、42a、および43aは、マスクaおよびbなどのマスクにより、データを

秘匿する。これにより、データ攪拌部において、左側32ビットのデータおよび右側32ビットのデータを外界から観測することが困難となる。しかし、上記マスクによるデータの秘匿を行った場合、図2の各S箱14への入力が本来の平文データのものとなる結果となる。したがって、各S箱14の出力も異なる結果、出力される暗号文が本来の平文データに対応したもので無くなる。

【0036】上記問題点を解消するために、各段の段関数においては、図4の排他的論理和25において、マスクbあるいはマスク b^{-} と排他的論理和を行う。これにより、図5aにおいて加えたマスクbまたは b^{-} による秘匿の影響を除去する。

【0037】さらに、スイッチSW12で0側の分岐の場合、排他的論理和32aにおいて、図5aで加えたマスクaによる秘匿の影響を除去する。すなわち、S29の入力は、本来の平文入力の場合と同じ入力となる。S29の出力は、排他的論理和33aにおいて、マスクaにより再び秘匿される。ここで、処理ブロック34aは事前計算によりテーブル参照で行われるので、外界から、S29の直接の入出力に関係した電力消費のデータの有意な変異を観測することはできない。

【0038】図4の排他的論理和24により、右側32ビットのデータに加えたマスクaあるいはマスク a^{-} の影響を一旦除去する。しかし、右側32ビットのデータは依然、マスクbあるいはマスク b^{-} により秘匿されているので安全である。右側32ビットのデータは次段の左側32ビットのデータになり、排他的論理和31において転置P30の出力と排他的論理和を行うことにより、再び、マスクa(あるいはマスク a^{-})およびマスクb(あるいはマスク b^{-})によって秘匿され、その次の段の右側入力となる。したがって、上述の通り、各段の各S箱における変換のDESとの同一性は保たれる。

【0039】また、最終段の出力においては、図5aにおいて加えた各マスクの秘匿の影響を除去するため、図5bに示した、各マスクによる排他的論理和を行う。

【0040】スイッチSW11、SW12、SW13、およびSW14は、乱数列 $\{R1i\}$ によって制御する。スイッチSW21、SW22、およびSW23は、乱数列 $\{R2i\}$ によって制御する。例えば、各スイッチは、 $R_{ji}=0$ のとき0側の分岐を、 $R_{ji}=1$ のとき1側の分岐を選ぶ。スイッチの制御を行う乱数列 $\{R1i\}$ および $\{R2i\}$ は、各ブロックの暗号化および復号の処理ごとに变化させることを特徴とする。例えば、ある暗号化の処理では各段のスイッチSW11、SW12、SW13、およびSW14はすべて0側で処理を行い、別の暗号化では、各段のスイッチSW11、SW12、SW13、およびSW14はすべて1側で処理を行う。

【0041】乱数列 $\{R1i\}$ と乱数列 $\{R2i\}$ に明白な依存関係があった場合、攻撃者にマスクaとマスクbを推測する手がかりを与えることになるので、乱数列

{R1i} と乱数列 {R2i} には明らかな依存関係を持たない乱数列を用いる。

【0042】理想的には、統計的に独立な2つの乱数列を用いることが推奨される。

【0043】ただし、実際には、統計的依存関係が存在しても、その影響が充分小さければ、DPA対策として有効である。本発明を実装する手段として2つのm系列生成器を用意して、第1のm系列生成器の出力を{R1j}、第2のm系列生成器の出力を{R2j}とすることが考えられる。m系列の周期が充分長く2つのm系列生成器の系列長、対応する規約多項式、初期値の一部または全部が異なるようにすれば上記条件を充分満たすと考えられる。連数列の別な実現手段として、1つのm系列生成器を用意し、それを1回の暗号化または復号の処理毎に2ビットを生成させ、その第1ビットを{R1j}、第2ビットを{R2j}として用いることが考えられる。

【0044】ここではm系列生成器を具体例として挙げたが、実用上安全と考えられる乱数列生成器なら何を用いても良い。なお、この乱数列が外部からは推測されない様に実装する必要がある。あるいは別な実現手段として、乱数列をあらかじめ記憶装置に蓄えておき、それを順次参照することも可能である。なお、この乱数列が外部からは推測されない様に実装する必要がある。

【0045】図4、図5a、および図5bにおいて、ビット列の1の数、すなわちハミング重みを $H(a)$ で定義する。DPAでは、データ暗号化処理に伴う消費電力の差異を観測して暗号化鍵に関する情報を収集する。上記マスクを用いたデータの隠蔽により、外界からの消費電力の計測と処理されるデータの対応をとることが困難となる。しかし、マスクのハミング重みに差異がある場合、複数の暗号化処理データの計測と統計情報により、マスクaとbのみを用いているデータのみを抽出することができる可能性がある。そして、そのようなデータのみ抽出が可能ならば、DPAの手法を用いることにより、従来の場合同様に鍵の抽出が可能となる。このように使用されているマスクがaなのかa'なのかの区別ができて充分な対策にならない。例えば、マスクaとa'あるいはマスクbとb'のハミング重みが同じとすれば、外界からの計測でマスクを判別することは困難となり安全であるが、逆に、マスクのビット重みに偏りがあるならば、安全性は著しく劣化する。

【0046】したがって、図4、図5a、および図5bにおいて、 $H(a) = H(a') = H(b) = H(b') = n/2 = 16$ の条件を満たすマスクの選択（以下、マスクのハミング重みが等しい）ならば安全性は高い。ここでマスクaおよびbのビット数nは32であるので、マスクa、マスクb、およびそれらのビット反転のビット重みがそれぞれ16であるマスク値を使用することが推奨される。ただし、理想的には上記のようにマスク

のハミング重みがマスクのビット長の丁度半分であるマスクを使用することが推奨されるが、ハミング重みがほぼ等しい2つのマスクを用い同様の効果が得られる。

【0047】すなわち、各マスクのハミング重みが極端に偏っていないければ、外界からの計測でマスクを判別することは容易でなく、DPA対策としての効果が得られる。

【0048】さらに、図4のDESの拡大転置26の特性に着目する。上記ハミング重みに着目したマスク値の選択と同様の理由から、排他的論理和32aおよび32bにおいて加えられる、 $E(a)$ と $E(a')$ のハミング重みが等しくなるマスクを選択する。すなわち、 $H(E(a)) = H(E(a'))$ を満足するマスクを選択する。

【0049】上記マスクの条件をDESの実装に当てはめると、例えばマスクaに対しては、マスクaを4ビットずつ区切ったときの各ブロックの“第1ビット”（左端のビット）の1の数＝マスクaを4ビットずつ区切ったときの各ブロックの“第4ビット”（右端のビット）の1の数＝4の条件を満たすことを要求する。すなわち、上記条件を満たすマスクaおよびマスクbの選択を特徴とする。上記条件を満たすマスク値の例として、 $(1000011111011011110010100100001)_2$ や $(11011010011001010011010110001010)_2$ などが使用できる。

【0050】ただし、理想的には上記条件を満たすマスク値を使用することが推奨されるが、「マスクaを4ビットずつ区切ったときの各ブロックの“第1ビット”の1の数」と「マスクaを4ビットずつ区切ったときの各ブロックの“第4ビット”の1の数」が、極端に偏っていないければ同様の効果が得られる。

【0051】なお、上記条件を満たすマスク値を使用する場合において、スイッチを制御する乱数列{R1j}と{R2j}が自明な相関を持たないならば、マスクaとマスクbが同一のマスク値であっても、DPA対策として有効である。

【0052】図1に示したDESの構成は最も広く知られているものであるが、処理の高速化をねらい、様々な等価変形を施したDESの構成法が知られている。

【0053】以下、本発明をDESに適用した場合における変形例について説明する。

【0054】図10はDESの等価変形の例である。図10に示すDESの実装においては、処理の効率化のために、拡大転置E11と転置P15を一つの転置にまとめEP53として処理している。入力された平文58を初期転置IP57において転置を行った出力は、二つに等分され、右側32ビットは拡大転置E51aに入力され、左側32ビットは拡大転置E51bに入力される。拡大転置E51aの出力48ビットは第一段の入力の右側48ビットである。拡大転置E51bの出力48ビットは第一段の入力の左側48ビットである。入力の右側48ビ

ットは排他的論理和55において、拡大鍵K1と排他的論理和が行われ、S箱54に出力される。S箱54はテーブル参照により対応する出力をEP53に出力する。EP53において、入力に転置が行われ、排他的論理和56に出力される。排他的論理和56において、拡大転置E51bの出力である左側48ビットと、EP53の出力の排他的論理和が行われ、次段の入力の右側48ビットになる。上記第1段の処理を第16段まで繰り返す。第16段の出力において、右側48ビットは縮約転置E⁻¹52aに入力され、左側48ビットは縮約転置E⁻¹52bに入力され、それぞれの出力32ビットは最終転置IP⁻¹59に入力され、64ビットの暗号文60が出力される。

【0055】このような変形版DESに本発明を適用し、DPAを防止する手法を以下に示す。

【0056】図11は図10で示したDESの実装に対する、本発明の一実施形態である。図11において、E(a)/E(a⁻)は図3に示した、排他的論理和によるスイッチSW23のマスクの加え方を表す。すなわち、E(a)/E(a⁻)はE(a)もしくはE(a⁻)によるマスクを表す。

【0057】図11は、図10で示したDESの実装に対しても、図4、図5a、および図5bで示した本発明の適用が可能であることを示す一実施形態である。

【0058】入力された平文に初期転置を行った出力は、二つに等分され、右側32ビットは拡大転置E61aに入力され、左側32ビットは拡大転置E61bに入力される。拡大転置E61aの出力48ビットは排他的論理和64において、マスクE(a)/E(a⁻)と排他的論理和が行われ、排他的論理和65に出力される。排他的論理和65において、排他的論理和64の出力はマスクE(b)/E(b⁻)と排他的論理和が行われ、第1段の入力の右側48ビットになる。なお、排他的論理和の性質により、排他的論理和64と65の順序を入れ替えても良い。

【0059】拡大転置E61bの出力48ビットは排他的論理和69において、マスクE(b)/E(b⁻)と排他的論理和が行われ、第1段の入力の左側48ビットになる。

【0060】入力の右側48ビットは、排他的論理和66において、マスクE(a)/E(a⁻)と排他的論理和が行われ、次段の入力の左側48ビットになる。入力の右側48ビットは、排他的論理和67において、マスクE(b)/E(b⁻)と排他的論理和が行われ、排他的論理和68に出力される。排他的論理和67の出力は、排他的論理和68において、拡大鍵K1と排他的論理和が行われ、S⁻62に出力される。S⁻62の構造については後述する。SS⁻62の出力はEP63により転置が行われ、排他的論理和70に出力される。

【0061】排他的論理和70において、入力データの

左側48ビットと、EP63の出力は排他的論理和が行われ、次段の入力の右側48ビットになる。上記第1段の処理を第16段まで繰り返す。最終段の出力においては、第1段への入力で述べた処理の逆を行う。すなわち、右側48ビットには排他的論理和65、排他的論理和64および縮約転置E⁻¹を行い、左側48ビットには排他的論理和65および縮約転置E⁻¹を行い、それぞれの出力32ビットづつを最終転置に出力する。

【0062】図12は図11に示したS⁻62の構造を示す図である。

【0063】図12において、 $\alpha = E(a)$ 、 $\alpha^- = E(a^-)$ と表す。S⁻62の入力は、排他的論理和71において、マスク α あるいはマスク α^- と排他的論理和が行われ、S箱72に出力される。S箱72の出力は、排他的論理和73において、マスクP⁻¹E⁻¹(α)あるいはマスクP⁻¹E⁻¹(α^-)と排他的論理和が行われ、S⁻62の出力となる。

【0064】すなわち、図12の74は、本発明においては図4に示したスイッチSW12およびスイッチSW11を含む、処理ブロック34aと34bに対応する。ただし、74の処理は、暗号化および復号の処理中に行ってはならない。なぜならば、上記マスクによるデータの秘匿を行っていても、S箱72の入出力は秘匿されていないため、S箱の処理による消費電力の差異を用いた解読が試みられる可能性があるからである。

【0065】本発明の実施形態においては、暗号化および復号を行う前に、事前計算により74の処理結果を作成し、暗号化および復号処理で使用することを特徴とする。例えば、各S箱について、S箱の入力のインデックスと出力を書き換えたテーブルを用意し、S⁻として暗号化および復号の処理に用いる。このとき、マスク α に対応したS⁻のテーブルとマスク α^- に対応したS⁻のテーブルがS箱に用意される。

【0066】図13はDESの等価変形の別の例である。

【0067】図13に示すDESの実装においては、処理の効率化のために、拡大転置E11と転置P15を一つの転置にまとめEP83として処理している。入力された平文88を初期転置IP87において転置を行った出力は、二つに等分され、右側32ビットは転置P⁻¹81aに入力され、左側32ビットは転置P⁻¹81bに入力される。転置P⁻¹81aの出力32ビットは第一段の入力の右側32ビットである。転置P⁻¹81bの出力32ビットは第一段の入力の左側32ビットである。入力の右側32ビットはEP83に入力され、拡大転置を行われた結果が排他的論理和85に出力される。排他的論理和85において、拡大鍵K1と排他的論理和が行われ、S箱84に出力される。S箱84はテーブル参照により対応する出力を排他的論理和86に出力する。排他的論理和86において、拡大転置E81bの出力である左側32ビットと、S箱84の出力の排他的論理和が行われ、

次段の入力の右側32ビットになる。上記第1段の処理を第16段まで繰り返す。

【0068】第16段の出力において、右側32ビットは転置P82aに入力され、左側32ビットは転置P82bに入力され、それぞれの出力32ビットは最終転置IP⁻¹89に入力され、64ビットの暗号文90が出力される。このような変形版DESに本発明を適用し、DPAを防止する手法を以下に示す。

【0069】図14は図13で示したDESの等価変形の例に対する、本発明の一実施形態である。

【0070】図14において、 $P^{-1}(a)/P^{-1}(a^-)$ は図3に示した、排他的論理和によるスイッチSW23のマスクの加え方を表す。すなわち、 $P^{-1}(a)/P^{-1}(a^-)$ は $P^{-1}(a)$ もしくは $P^{-1}(a^-)$ によるマスクを表す。

【0071】図14は、図13で示したDESの実装に対しても、図4、図5a、および図5bで示した本発明の適用が可能であることを示す一実施形態である。

【0072】入力された平文に初期転置を行った出力は、二つに等分され、右側32ビットは転置P⁻¹91aに入力され、左側32ビットは転置P⁻¹91bに入力される。転置P⁻¹91aの出力32ビットは排他的論理和94において、 $P^{-1}(a)/P^{-1}(a^-)$ と排他的論理和が行われ、排他的論理和95に出力される。排他的論理和95において、排他的論理和94の出力はマスク $P^{-1}(b)/P^{-1}(b^-)$ と排他的論理和が行われ、第1段の入力の右側32ビットになる。転置P⁻¹91aの出力32ビットは排他的論理和94において、マスク $P^{-1}(b)/P^{-1}(b^-)$ と排他的論理和が行われ、第1段の入力の左側32ビットになる。なお、排他的論理和の性質により、排他的論理和94と95の順序を入れ替えても良い。

【0073】入力の右側32ビットは、排他的論理和96において、マスク $P^{-1}(a)/P^{-1}(a^-)$ と排他的論理和が行われ、次段の入力の左側32ビットになる。入力の右側32ビットは、排他的論理和97において、マスク $P^{-1}(b)/P^{-1}(b^-)$ と排他的論理和が行われ、EP93に出力される。EP93において拡大転置を行った結果の48ビット出力は、排他的論理和98に出力され、拡大鍵K1と排他的論理和が行われ、S⁻92に出力される。S⁻92の構造については後述する。S⁻92の出力は、排他的論理和100に出力され、入力データの左側32ビットと、排他的論理和が行われ、次段の入力の右側32ビットになる。上記第1段の処理を第16段まで繰り返す。

【0074】最終段の出力においては、第1段への入力 で述べた処理の逆を行う。すなわち、右側32ビットには排他的論理和95、排他的論理和94および転置Pを行い、左側32ビットには排他的論理和95および転置Pを行い、それぞれの出力32ビットづつを最終転置に

出力する。

【0075】図15は図14に示したS⁻92の構造を示す図である。

【0076】図15において、 $\alpha = P^{-1}(a)$ 、 $\alpha^- = P^{-1}(a^-)$ と表す。

【0077】S⁻92の入力は、排他的論理和101において、マスク α あるいはマスク α^- と排他的論理和が行われ、S箱102に入力される。

【0078】S箱102の出力は、排他的論理和103において、マスク $P^{-1}E^{-1}(\alpha)$ あるいはマスク $P^{-1}E^{-1}(\alpha^-)$ と排他的論理和が行われ、S⁻92の出力となる。すなわち、図15の104は、本発明においては図4に示したスイッチSW12およびスイッチSW11を含む、34aと34bに対応する。ただし、104の処理は、暗号化および復号の処理中に行ってはならない。なぜならば、上記マスクによるデータの秘匿を行っていても、S箱102の入出力は秘匿されていないため、S箱の処理による消費電力の差異を用いた解説が試みられる可能性があるからである。すなわち、本発明の実施形態においては、暗号化および復号を行う前に、事前計算により104の処理結果を作成し、暗号化および復号処理で使用することを特徴とする。例えば、各S箱について、S箱の入力のインデックスと出力を書き換えたテーブルを用意し、S⁻として暗号化および復号の処理に用いる。

【0079】このとき、マスク α に対応したS⁻のテーブルとマスク α^- に対応したS⁻のテーブルがS箱に用意される。

【0080】次に、図16、図17、および図18を用いて本発明を鍵スケジュール部に適用した一実施形態を説明する。

【0081】真の鍵のビットパターンKをマスクするマスクパターンcとそのビット反転パターン c^- を用意し、Kを指定された2項演算を用いてcによって変換した値をKcとし、また同じ2項演算を用いてKを c^- によって変換した値をK c^- とし、KcとK c^- をあらかじめ記憶装置に記憶しておき、暗号化または復号を実施する度にランダムにKcとK c^- の一方を選択し、それを真の鍵と同様の処理によって処理し、平文に対して前記2項演算によって作用させると共に、その2項演算の出力からcまたは c^- の対応するパターンの影響を前記2項演算の逆変換により除去する。2項演算として排他的論理和を用いる暗号方式の例としてDES方式に本発明を適用した場合の例を示す。まず、鍵KcとK c^- の2つのマスクされた鍵を用意する。

【0082】 $Kc = K (+) c$

$Kc^- = K (+) c^-$

但し、記号(+)はビット毎の排他的論理和を表す。

【0083】暗号化または復号に先立ってまずKc、K c^- のいずれか一方をランダムに選択し、DESの鍵スケ

ジュール処理を行い、順次16通りの拡大鍵を生成する。Kcから拡大された16個の鍵は記号Kci ($i=1, \dots, 16$) で表し、Kc⁻から拡大された鍵はKc⁻i ($i=1, \dots, 16$) であらわす。Kcから拡大された拡大鍵はマスクcの影響を、またKc⁻から拡大された拡大鍵はマスクc⁻の影響をそれぞれ受けている。その影響はDESの鍵スケジュール処理により定まるが、ここでは、マスクを掛けていない真の鍵Kを鍵スケジュールで拡大した鍵をKi ($i=1, \dots, 16$) と表し、KiとKciの排他的論理和をciとし、KiとKc⁻iの排他的論理和をc⁻iとする。すなわち $ci = Ki (+) Kci$

$$c^{-}i = Ki (+) Kc^{-}i$$

DESにおいて各拡大鍵Kiは拡大転置Eの直後にビット毎の排他的論理和演算によってメッセージに作用させられる。本発明においては、Kiの代わりにKciまたはKc⁻iを作用させる。Kciを作用させた場合にはKciを作用させた後に、ciを排他的論理和によって作用させてその影響を取り除き、Kc⁻iを作用させた場合にはc⁻iを作用させた後に、排他的論理和演算で作用させその影響を取り除く。ci、c⁻iはそれぞれcおよびc⁻をDESの鍵スケジュールで拡大鍵同様に拡大することによって得られる。ciやc⁻iは暗号化または復号の度に選択されたマスクcまたはc⁻から作成してもよい。但し、外部からの観測に対して最も漏洩する情報が少ない方法は、あらかじめciとc⁻iをすべて計算しておくことである。その場合、48ビットのマスク16通りを2セット、合計1536ビットあらかじめ用意することになる。このマスクは例えばICカードに本発明を適用した場合、少なくともカード毎固定で良いので、ci、c⁻iはROMに書き込んでおくことができる。このことはメモリ量の制約が強いICカードにおいては特に重要である。一般に同じビット数を記憶する場合、RAMやEEPROMに比べROMの面積は小さい。従って1536ビットのマスクをROMに記憶させることはRAMやEEPROMに記憶させるのに比べLSIチップ面積の使用効率が高くなる。

【0084】図16にDESの鍵スケジュールを示す。

【0085】図中(PC-1)111と(PC-2)113はビットの選択と転置を組み合わせた関数であり、記号ROT112は巡回シフト演算を表す。外部から入力された64ビットの鍵K115は(PC-1)111により、その内8ビットが捨てられ、28ビットの2つのビット列が巡回シフト112に渡される。巡回シフトされた合計56ビットのデータはPC-2変換113に入力され、拡大鍵48ビットが出力される。図では1段分の拡大鍵のみ出力しているが、巡回シフトとPC-2を繰り返すことによって2、3、...、16段の拡大鍵を生成する。

【0086】図17は鍵スケジュール部に本発明を適用

した場合の処理の流れを表している。

【0087】鍵スケジュールの鍵入力段ではスイッチSW31により、KcとKc⁻からランダムにほぼ1/2の確率で選択し、鍵スケジュール部122に入力される。以下の鍵スケジュール部内での処理は通常のDESの鍵スケジュール処理と同じである。出力される拡大鍵123は入力された鍵がKcであれば、Kci、Kc⁻の時にはKc⁻iとなる。

【0088】図18はマスクの影響を受けた拡大鍵を各ラウンド関数においてメッセージに作用させる様子を示している。

【0089】KciまたはKc⁻iの一方をメッセージに作用させる方法は、通常の場合Kiを作用させるのと同様であり、拡大転置E131の出力48ビットに、排他的論理和132において拡大鍵KciまたはKc⁻iをビット毎の排他的論理和演算によって作用させる。こうして作用させた結果はマスクcまたはc⁻の影響を受けているのでこのままS箱に入力させると正しい暗号変換ができなくなる。従ってS箱に入力する前にマスクcまたはc⁻の影響を取り除く処理が必要である。具体的にはマスクの影響がciの場合、ciを排他的論理和133によってS箱134の入力前に作用させる。排他的論理和の逆変換は排他的論理和であるので、これによってciの影響が除去できる。マスクの影響がc⁻iの場合も同様である。

【0090】本実施形態においてマスクc⁻はマスクcのビット反転に選べば、拡大鍵の各ビットは1と0の値をほぼ均等に採る。これによって、暗号装置外部からの種々の観測に対して鍵に関する情報の漏洩を無くすることができる。漏洩する情報をできる限り少なくするには、さらにciとc⁻iのハミング重みが近い値をとることが望ましい。但しciはcを鍵スケジュールに通した結果であり全ての段のciのハミング重みを完全にコントロールすることは困難である。そこで、例えば元のマスクcのハミング重みがビットサイズの1/2であるように選ぶ方法が考えられる。

【0091】上述した実施形態においては、DES方式への適用について詳しく述べたが、本発明はこれに限らず、排他的論理和の様な2項演算、ビット入れ替えに相当する転置、S箱に相当する換字の3種の一部または全部を使用して構成される様な暗号方式全般に適用可能である。

【0092】

【発明の効果】本発明によれば、与えられた暗号化および復号処理の同一性を保証しつつ、DPAによる解読を困難にすることにより、DPAに対する安全性を増大することができる。

【図面の簡単な説明】

【図1】DESアルゴリズムの全体構成を示す図。

【図2】DESの段関数の構成を示す図。

【図3】DESの規格表に従うS箱の内容の一例を示す図。

【図4】本発明による段関数にマスクを加えた構成を示す図。

【図5】本発明による入力段及び最終段でマスクを加えた構成を示す図。

【図6】拡大転置Eの表を示す図。

【図7】転置Pの表を示す図。

【図8】マスクaの場合、入力が(000000、000001、…111111)に対応する隠蔽されたS1の出力を示す図。

【図9】マスクa- (aのビット反転)のテーブルを示す図。

【図10】DES アルゴリズムの一実装例の構成を示す図。

【図11】図10の構成において、本発明による段関数にマスクを加えた構成を示す図。

【図12】図11のS^{*}の構成を示す図。

【図13】DES アルゴリズムの別の一実装例の構成を示す図。

【図14】図13の構成において、本発明による段関数にマスクを加えた構成を示す図。

【図15】図14のS^{*}の構成を示す図。

【図16】DES アルゴリズムの鍵スケジュール部の構成を示す図。

【図17】本発明による鍵スケジュール部にマスクを加える構成を示す図。

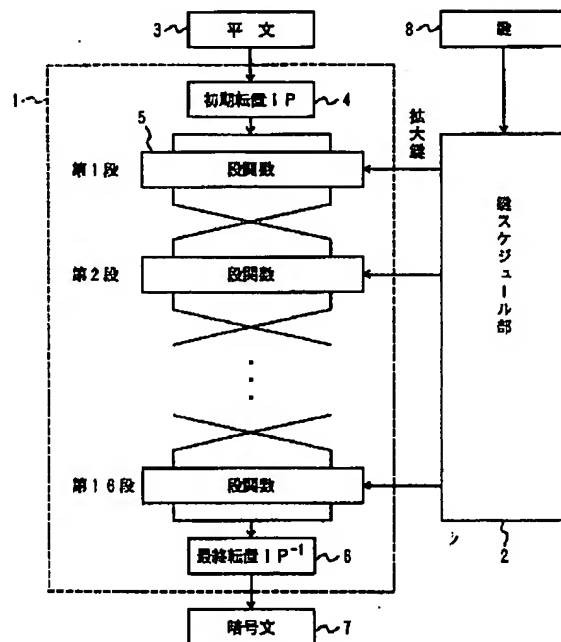
【図18】本発明による段関数に鍵スケジュール部で加

えたマスクを加える構成を示す図。

【符号の説明】

- 1…データ攪拌部
- 2…鍵スケジュール部
- 3…平文
- 4…初期転置IP
- 5…段関数
- 6…最終転置IP⁻¹
- 7…暗号文
- 8…鍵
- 11…拡大転置E
- 12…拡大鍵
- 13…排他的論理和
- 14…S箱
- 15…転置P
- 16…排他的論理和
- 17…段関数
- 24、25、27、31、32a、32b、33a、33b…排他的論理和
- 26…拡大転置E
- 29…S箱
- SW11、SW12、SW13、SW21、SW22、SW23…スイッチ
- 34a、34b…処理
- 42a、43a、44a、42b、43b、44b…排他的論理和
- 41a…初期転置IP
- 41b…最終転置IP⁻¹

【図1】

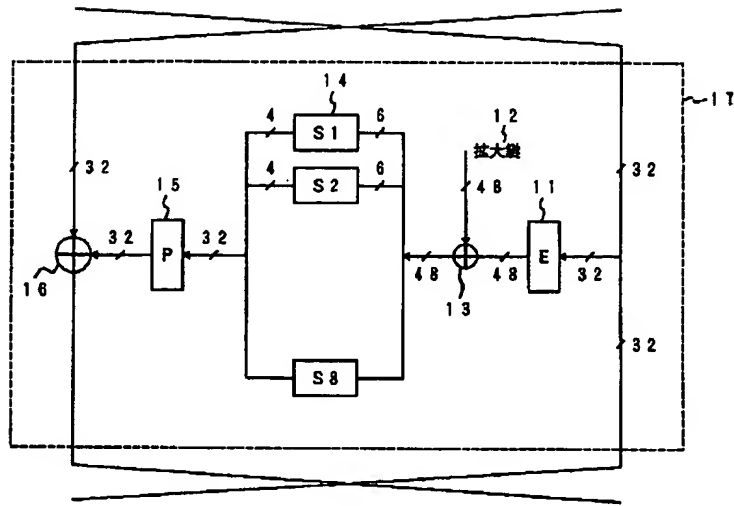


【図6】

拡大転置Eの表

32, 1, 2, 3, 4, 5
4, 5, 6, 7, 8, 9
8, 9, 10, 11, 12, 13
12, 13, 14, 15, 16, 17
16, 17, 18, 19, 20, 21
20, 21, 22, 23, 24, 25
24, 25, 26, 27, 28, 29
28, 29, 30, 31, 32, 1

【図2】

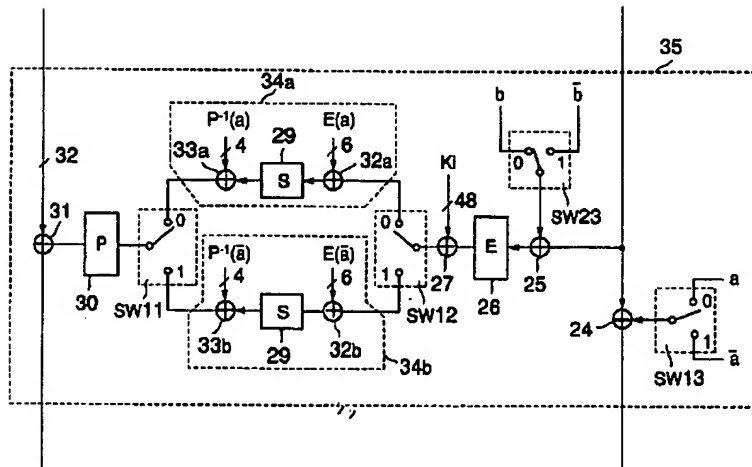


【図3】

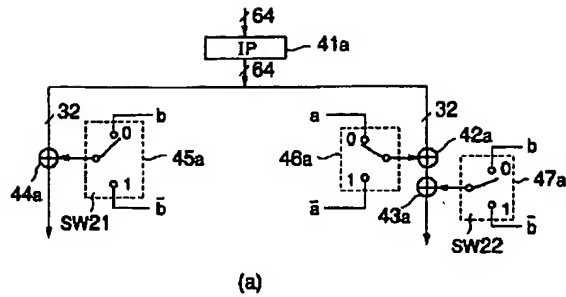
S1の表

14, 4, 13, 1, 2, 15, 11, 8, 3, 10, 6, 12, 5, 9, 0, 7,
 0, 15, 7, 4, 14, 2, 13, 1, 10, 6, 12, 11, 9, 5, 3, 8,
 4, 1, 14, 8, 13, 6, 2, 11, 15, 12, 9, 7, 3, 10, 5, 0,
 15, 12, 8, 2, 4, 9, 1, 7, 5, 11, 3, 14, 10, 0, 6, 13,

【図4】



【図5】

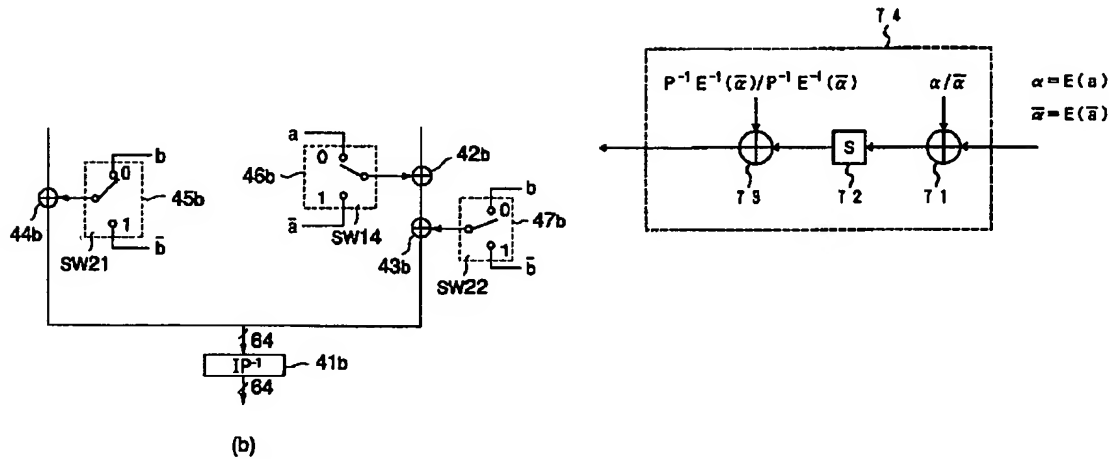


【図7】

転置Pの表

16, 7, 20, 21, 29, 12, 28, 17, 1, 15, 23, 26, 5, 18, 31, 10,
2, 8, 24, 14, 32, 27, 3, 9, 19, 13, 30, 6, 22, 11, 4, 25

【図12】



【図8】

マスクaの場合の、入力が(000000, 000001, ..., 111111)に
対応する隠蔽されたS1の出力

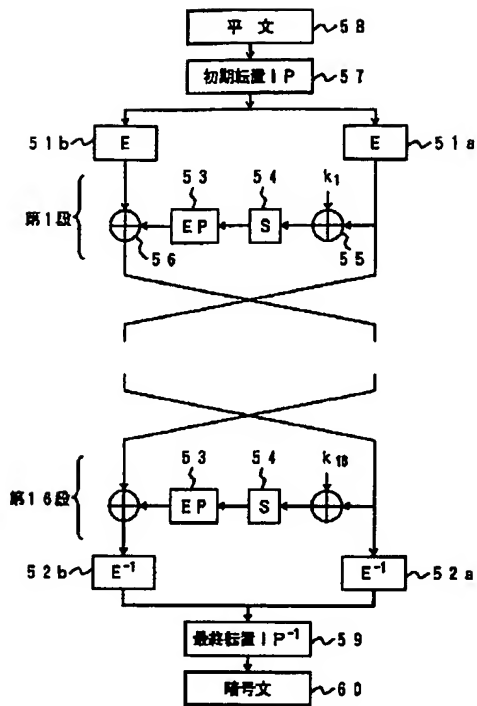
8 11 14 2 13 4 0 15 1 7 11 1 6 13 5 8 15 12 4 9 3 10 9
3 10 0 7 14 12 6 2 5 4 2 8 1 7 11 11 6 14 4 13 8 9 7 6
13 10 9 1 14 0 12 12 0 5 15 2 5 3 10 15 3

【図9】

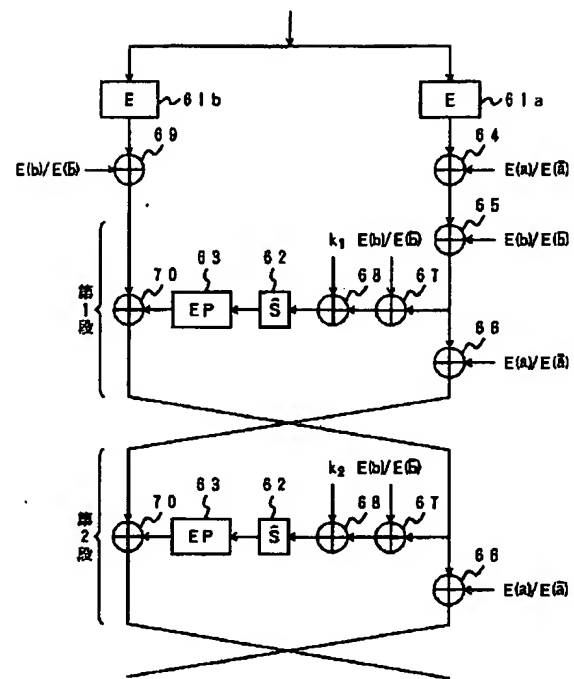
マスク \bar{a} (aのビット反転) のテーブル

12 0 5 12 10 13 0 10 15 3 3 15 1 14 6 5 2 9 8 6 7 2 11 1 9 4 4 8 14 7 13 11 10 1
3 9 3 1 8 15 5 12 6 5 12 6 11 3 0 7 10 2 9 14 4 8 14 0 15 11 2 13 1 4 7

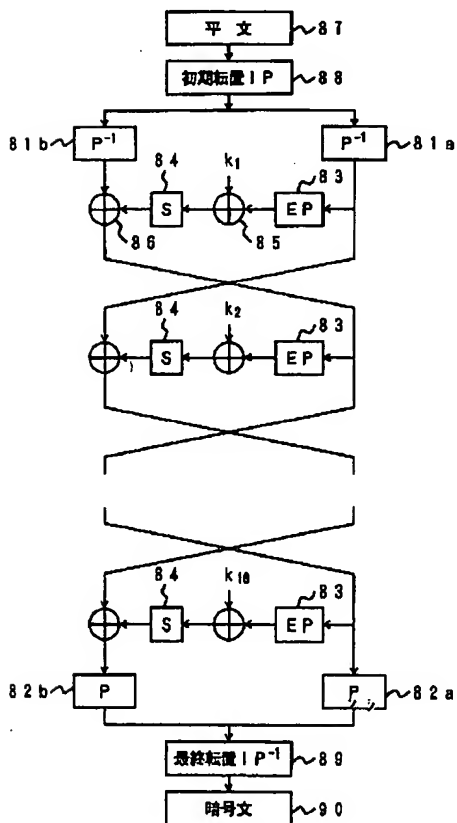
【图10】



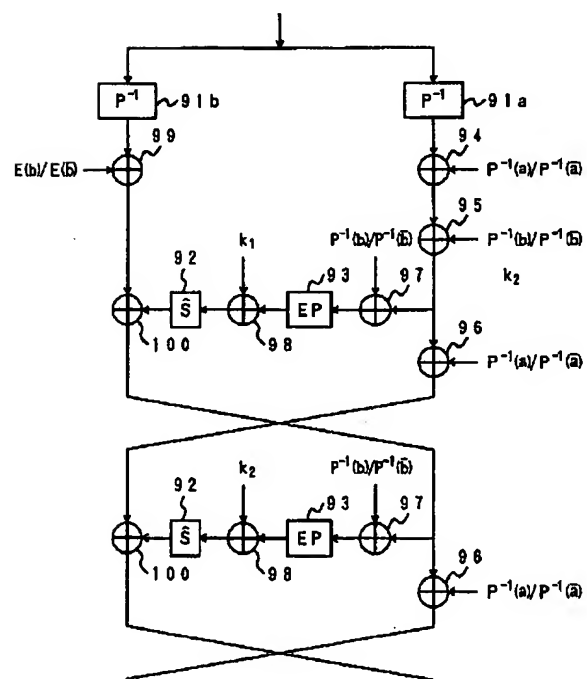
【图11】



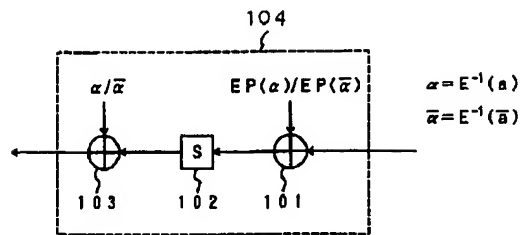
【图13】



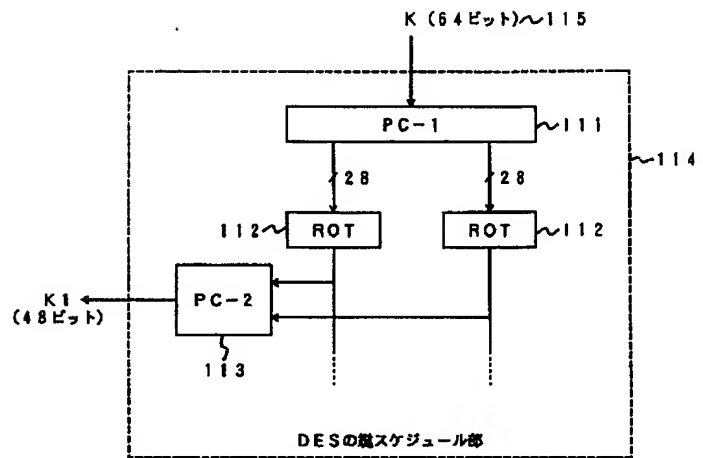
【图14】



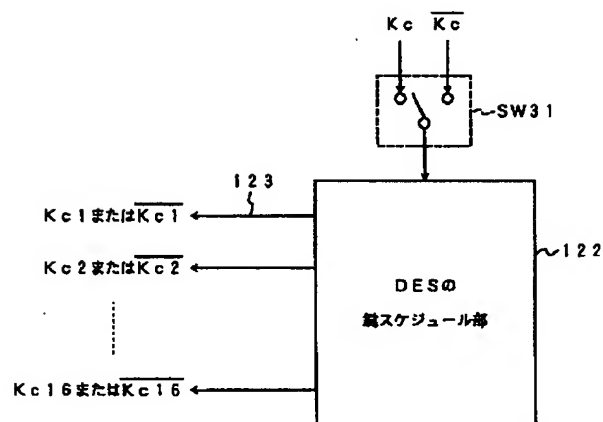
【図15】



【図16】



【図17】



【図18】

